ОСОБЕННОСТИ РЕАЛИЗАЦИИ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ НА ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМАХ

Караман Д.Г.
Национальный технический университет «Харьковский политехнический институт», г. Харьков,
E-mail: karaman@kpi.kharkov.ua

Физически неклонируемая функция (ФНФ) – это функциональная структура, у которой в процессе реализации за счет особенностей выбранного физического базиса для реализации могут произвольно изменяться реализуемые функциональные зависимости, причем каждая последующая реализуемая копия всегда будет иметь отличия от предыдущих своих реализаций. Такие функции просто оценить, но трудно охарактеризовать, а главное – трудно смоделировать и воспроизвести.

В физической структуре неклонируемой функции есть определенное множество компонентов, функциональная характеристика которых может произвольно изменяться в ходе производственного процесса. Если таких компонентов в реализуемой функции достаточно много, а функциональный параметр достаточно вариативный, то вероятность получения двух абсолютно идентичных физически неклонируемых функциональных структур оказывается очень низкой.

В последнее время исследованию методов построения и реализации ФНФ посвящено достаточно много научных работ, поскольку эти функции постепенно находят применение во многих сферах информационной и криптографической безопасности: смарт-карты, токены и банковские карты, защита физических носителей информации, интегральных схем от клонирования, генераторы случайных (псевдослучайных) чисел, генераторы криптографических ключей и т.д.

В работе [1] приведен основательный обзор различных тем, связанных с проектированием и оценкой ФНФ, в подробностях рассмотрены различные подходы к их реализации. Кроме того, авторы подробно рассматривают процесс реализации ФНФ на интегральных схемах.

В ФНФ могут использоваться различные источники физической случайности. Различают ФНФ, в которых случайность вносится внешними факторами: температурой, давлением, концентрацией примесей в рабочих материалах, а также ФНФ, в которых случайность проявляется в виде одного из свойств, внутренне присущих выбранному физическому базису: временем распространения сигнала, изменением уровня электрических потенциалов, проводимости и т.д.

Различают несколько основных технологий, с помощью которых можно получить ФНФ: оптическое зондирование (сканирование случайной интерференционной картины), инъекция диэлектрика (создание массива конденсаторов со случайными значениями емкостей), полупроводниковая матрица (использование случайности временных задержек в полупроводниках при изменении концентрации примесей) и магнитная (неравномерность свойств и степени намагничивания магнитного материала).

Все эти технологии являются ресурсо- и энергоемкими при реализации, требуют особых условий производства и серьезных научных, технических и материальных затрат на отработку технологии.

В связи с этим в ряде научных работ [2-6] была рассмотрена возможность реализации ФНФ на программируемых логических структурах, к которым относятся и программируемые логические интегральные схемы.

В докладе рассматриваются основные принципы реализации ФНФ на программируемых логических интегральных схемах типа FPGA, методы и принципы реализации ФНФ на конфигурируемых логических блоках. Сделан акцент на основных сложностях, которые возникают при проектировании, верификации получаемых решений, а также представлены основные направления дальнейшего развития представленных решений.

Список литературы

1. Christoph Böhm, Maximilian Hofer. Physical Unclonable Functions in Theory and Practice — Springer Science & Business Media, 2012. — 270 p. (ISBN: 9781461450399)

2. R. Maes and I. Verbauwhede, "Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions." // Towards Hardware-Intrinsic Security, ser. Information Security and Cryptography. Berlin Heidelberg: Springer, 2010, pp. 3-37.

3. Durga Prasad Sahoo, Sayandeep Saha, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, Hitesh Kapoor, “Composite PUF: A new design paradigm for Physically Unclonable Functions on FPGA.” // IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), — 2014.

4. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "Extended abstract: The buttery PUF protecting IP on every FPGA," in Proc. of IEEE Int. Symposium on HOST , June 2008, pp. 67-70.

5. H. Yu, P. H. W. Leong, and Q. Xu, "An FPGA Chip Identication Generator Using Congurable Ring Oscillators," IEEE Trans. VLSI Syst., vol. 20, pp. 2198-2207, 2012.

6. M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for Design and Implementation of Secure Recongurable PUFs," ACM Trans. Recongurable Technol. Syst., vol. 2, no. 1, pp. 1-33, 2009.